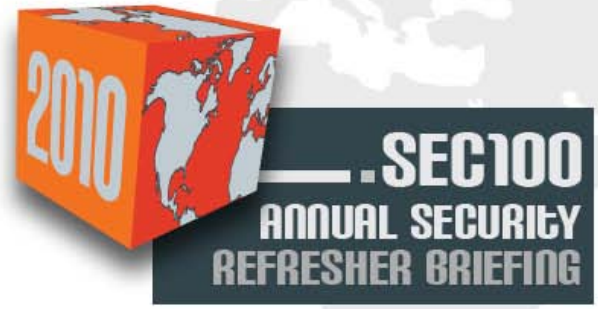

2010
.SEC100
ANNUAL SECURITY
REFRESHER BRIEFING

Overview

Welcome to the 2010 Annual Security Refresher Briefing (SEC100). This briefing must be completed by all cleared Members of the Workforce. As DOE requires, the annual security refresher briefing addresses site-specific issues and selectively reinforces other information provided in the Comprehensive Briefing (SEC150). This year's SEC100 focus is security incidents, the problems associated with those incidents, and your responsibilities for preventing such incidents.

Security incidents can result in compromise of classified or sensitive information, and they have a significant negative impact on Sandia's reputation. We must be aware of our security responsibilities, and dedicate ourselves to taking precautions to prevent security incidents. We must also take the initiative to immediately report incidents of concern so that a determination can be made as to its severity and what action is needed to mitigate the situation.

Members of the Workforce are the "eyes and ears" of Sandia security. Stay alert as you go about your daily business, and report anything that does not look or seem right.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000

Table of Contents

Instructions

How to Receive Credit

- Read through all course modules.
- Answer all end-of module practice questions.
- E-mail SEC100 Completion Record to SecurityEd@sandia.gov or fax to (505) 284-6079 for credit.

Completion Time

Course completion time is estimated to be between 30-40 minutes. However, course completion times vary greatly, depending upon familiarity with the content, reading speed, number of interruptions, and number of optional links accessed. A course session will remain open for 15 days.

Employees may charge up to 30 minutes to A-290 for their time to complete this training.

Resources

Corporate Policy System and External Source Requirements Documents

- HR100.4.6, *Prevent and Test for Workplace Substance Abuse*
- IM100.1, *Use and Protect Information Technology Resources*
- ISS100.1, *Perform Classified Work*
- ISS100.3.1, *Report Personnel Security Information; Security Incidents; and Waste, fraud, and Abuse*
- ISS100.4.1, *Control Access by Foreign Nationals to Unclassified DOE Information, Programs, and Technologies, and SNL Sites*
- ISS100.4.3, *Comply With Export/Import Controls*
- ISS100.5.2, *Conduct and Report Technical Surveillance*
- ISS100.5.3, *Control Site Access*
- ISS100.5.4, *Manage Clearances*
- ISS100.5.5, *Use, Control, and Protect Badges*
- DOE M 470.4-1, Section K, "Safeguards and Security Awareness Programs"
- Title 10, *Code of Federal Regulations*, Part 824 (10 CFR 824), "Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations"

Websites

- Badge Office website
- California Site Operations Center (8500) Security homepage
- Classification Office's DC Access List
- Clearance Office
- Corporate Investigations website
- DOE Sensitive Countries List
- Foreign Interactions website
- Host Certification and Risk Assessment
- Laptops on Foreign Travel (LOFT) website
- OOPS, A Reporting Guide
- Physical Security and Planning website
- Safeguards and Security (S&S) website

- S&S Lessons Learned website
- Technical Surveillance Countermeasures (TSCM) website

Course Contact

For Questions	Contact:
Course Administrator & Program Owner	Fran Armijo **fparmij@sandia.gov**, (505) 284-2416, MS-1341

SEC100 Completion Record

After reading all the modules and answering the module practice questions in SEC100, Annual Security Refresher Briefing, fill in the form below and forward to the Course Administrator by e-mail SecurityEd@sandia.gov or fax to (505-284-6079) in order to receive course credit.

I have read all the modules and answered all the practice questions in SEC100 Annual Security Refresher Briefing.

Print Full Name (Last, First, Middle)	
SNL org. or Company Name	
Signature	Date

☐Employee ☐Contractor ☐Consultant

☐Student ☐KMP

If you would like confirmation of your completion, provide either:

☐ _____

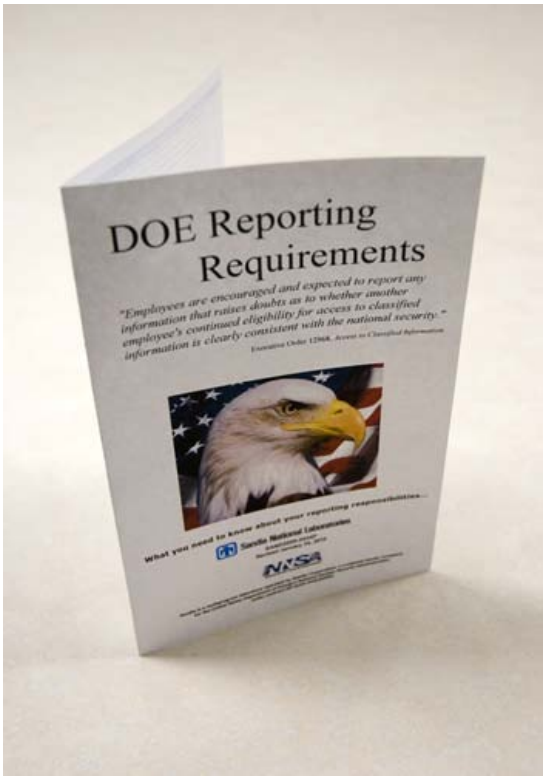
Email Address (Please write legibly)

☐ _____

Fax Number

Module 01 - Reporting Requirements

Objectives
After completing this module, you should be able to identify the key personal information for which you and management bear reporting responsibilities.



Goals
Sandia is committed to maintaining a security-conscious culture in which access to vital national security facilities and information is recognized as a privilege. Maintaining that privilege requires each individual to fully understand and fulfill the security obligations associated with his or her clearance (a.k.a. "access authorization").

Reporting requirements are significant obligations that each cleared individual must implement. Generally, this involves both an oral and a written report. However, time requirements differ for each, as outlined in the DOE Reporting Requirements Matrix.

Your Responsibilities
Violations of the Law Within or Outside of the United States
If you are arrested, subject to criminal charges (including charges that are dismissed), or are detained by federal, state, or other law-enforcement authorities, report to:

- NM: Corporate Investigations (505-845-9900)
- CA: Clearance Processing (925-294-2061)

Traffic violations for which only a fine of **$250.00 or less** was imposed do **not** have to be reported, unless the violations were drug or alcohol related. Refer to the DOE Reporting Requirements Matrix for additional details on reporting traffic violations.

Contacts with Foreign Nationals
You must immediately report substantive contact with any foreign national.

Note: Contact is defined as "a substantive professional or personal relationship other than family members." Substantive is defined as "a relationship that is enduring, involves substantial sharing of personal information and/or the formation of emotional bonds."

Drugs and Intoxicants
Illegal drugs are prohibited on Sandia-controlled premises. The use of illegal drugs is a serious offense and could result in termination of your clearance and, eventually, your employment, as well as arrest.

Incidents of illegal drugs must be reported to (NM) Corporate Investigations (505-845-9900) or (CA) Security Operations (925-294-2531). This includes, but is not limited to, trafficking, selling, transferring, possessing, or using illegal drugs. Individuals who illegally used or trafficked a controlled substance may be asked to sign a drug certification form attesting to their commitment to refrain from using or being involved with illegal drugs while employed in a position requiring a security clearance.

Note: You are not precluded from reporting information directly to the DOE Personnel Security Department.

Travel
You are required to report the following travel:

- Business-related travel to a sensitive country.
- Business-related travel to a non-sensitive country.
- Personal foreign travel to a sensitive country.

Such travel must be reported to the following:

- Business-related Travel to a Foreign Country: International Travel Help Line (505-845-1300)
- Personal Travel to a sensitive country: Enter travel into the Travel Information System (TIS)

Note: While you are not required to report personal foreign travel to a non-sensitive country, you should keep a personal record of such travel for future clearance (re)investigations.

Hospitalization
You or your manager must report when you are hospitalized for mental illness, or other condition (e.g., drug or alcohol abuse) that may cause significant defect in your judgment or reliability. NM reports must be made to Corporate Investigations (505-845-9900); CA reports must be made to Clearance Processing (925-294-2061).

Additional Reporting Requirements
Refer to the DOE Reporting Requirements Matrix for information regarding the following reporting requirements:

- Bankruptcy
- Wage garnishment
- Citizenship changes
- Name change
- Marriage and cohabitation
- Clearance termination
- Derogatory information
- Waste, fraud, and abuse

Individuals with SCI Clearances have additional reporting requirements and should contact their Special Security Office for details.

Resources

- ISS100.3.1, *Report Personnel Security Information; Security Incidents; and Waste, Fraud, and Abuse*
- Corporate Investigations website
- HBE Behavioral Health Program website
- Facility Security Officers (FSO) Toolcart (external website for contractors and consultants)
- DOE Sensitive Contries List

End of Module Question

Traffic violations for which a fine of $250.00 or less was imposed must be reported when the violations are drug or alcohol related.

a) True
b) False

Answer: a) True. Traffic violations for which a fine of $250.00 or less was imposed must be reported when the violations are drug or alcohol related.

Module 02 - Security Incident Management Program (SIMP)

Objective
After completing this module, you will be able to list causes of incidents of security concern and your role in reporting them.

Security Incidents at Sandia
In FY09, there were 1,408 reports of security concerns submitted to the Security Incident Management Program (SIMP). Of those, 657 resulted in security incidents. The majority of those security incidents were associated with controlled articles—generally electronic devices, such as cell phones, Bluetooth devices, Blackberry devices, and iPods. The other security incidents involved improperly secured classified vault-type rooms (VTRs) and classified repositories, e-mails, access controls, foreign interactions, improper handling (e.g., storage, use, or shipping) of classified matter, and unclassified events, such as protection of Unclassified Controlled Nuclear Information (UCNI).

Role of SIMP
SIMP was created to fulfill DOE's requirement that each site have an Incident of Security Concern program to provide "timely identification and notification of, response to, inquiry into, reporting of, and closure action for incidents of security concern." Such incidents are defined as actions, inactions, or events that can be categorized within any or all of the following criteria:

- Pose threats to national security interests and/or critical DOE assets.
- Create potentially serious or dangerous security situations.
- Degrade the effectiveness of the Safeguards and Security (S&S) program.
- Adversely affect the ability of organizations to protect DOE S&S interests.

SIMP is staffed by individuals known as Inquiry Officials (IO). Their mission is to conduct inquiries into incidents of security concern, determine whether a security incident has occurred based on the evidence, and report all security incidents to DOE within the required timeframe.

Causes of Security Incidents
Security incidents generally appear to be caused by one of four factors:

- Distractions – Interruptions that draw attention away from established processes.
- Complacency – Not taking an active interest in doing things right.

- Presumptions – The belief that something is right based on previous experience or knowledge.
- Change in routine.

Security incidents are categorized according to an Impact Measurement Index (IMI-1 thru IMI-4), based on their potential to cause serious damage or place S&S interests and activities at risk. IMI-1 is the highest risk category.

Your Responsibilities

Immediately notify SIMP about incidents of security concern:

- NM: Call 505-540-2382 (24/7 pager number)
- CA: Call 925-294-3238 (direct line) or 1-888-932-9710 (24/7 pager)

Do not discuss details pertaining to a security incident over unsecured lines. Request that an IO meet you at your location.

Also immediately report security concerns to your manager, so that the incident may be reported through OOPS (311). If your manager is unavailable, contact another member of management or call the OOPS number yourself.

Note: Contractors should also ensure that their company Facility Security Officer (FSO) is notified about the incident.

Take precautions to avoid creating a security incident. Use the Integrated Safeguards & Security Management (ISSM) principles (plan work, evaluate risk, implement controls, perform work, and improve process) when working with classified matter. Additional precautions include:

- Don't allow distractions or time pressures to keep you from following an established process.
- Don't become complacent about your security responsibilities.
- Don't presume that you know all the answers or have the latest information. Seek assistance.

Resources

- ISS100.3.1, *Report Personnel Security Information; Security Incidents; and Waste, Fraud, and Abuse*
- SIMP homepage
- OOPS

End of Module Question

Joanne believes that a security incident involving an escorted visitor may have occurred, but she's not sure. What action should Joanne take?

a) None, since she's not sure an incident occurred.
b) Report the incident to her Sandia manager and **ensure** SIMP is also notified.
c) Document the incident in a logbook in case someone else reports it.

Answer: b) Joanne should report the incident to her Sandia manager and ensure SIMP is also notified.

Module 03 - Classification

Objective
After completing this module, you will be aware of the issues and requirements involving classification, and your responsibilities for obtaining guidance from a Derivative Classifier (DC).

Security Incidents
In FY09, there were 50 security incidents that occurred due to failure to seek appropriate classification guidance. A few examples follow:

- A classified document that had been submitted for formal review and approval through Sandia's online process was originally identified as Official Use Only (OUO), based on outdated classification guidance.
- Open-source information presumed to be unclassified was inserted in a report.
- Compilation of unclassified information on what began as an unclassified e-mail correspondence resulted in classified content.
- Unclassified information obtained from Sandia's photo archives was elaborated upon, and thus became Export Control Information (ECI).

Your Responsibilities
Failure to seek proper classification guidance can result in the unauthorized and inadvertent disclosure of classified matter. Information that describes capabilities of systems, installation, infrastructures, projects, plans, or protection services relating to national security must be reviewed and protected appropriately to prevent compromise.

- Do not confirm or deny public statements concerning potentially classified information. Accidental release does not mean that a document or material has been declassified.
- Do not assume that all open-source information or old information is unclassified.
- Do not elaborate on information you obtain from any source without consulting with a DC.

You must also:

- Ensure that each document (e.g., project papers, e-mail, journal articles) generated in a classified subject area is reviewed by a DC when it moves beyond the "draft" stage.
- Have a document reviewed even if you only suspect that the document may contain classified and/or sensitive information. Consult your DC to avoid associating or compiling unclassified information that may result in a classified document.
- Send any document incorporating pictures from Sandia's photo archives through official Review and Approval.

If you think there are inconsistencies between the content of the document and its classification, appeal to the appropriate DC. Note that downgrade determinations require review by a Derivative Declassifier (DD) from the Classification Office (NM Department 4225 or CA Department 8511).

Manager Responsibilities

Managers whose organizations generate—or have the potential to generate—classified information must ensure that members of their organization complete CLA102, *Classified Programs Initial Awareness Briefing*, which is the first in the new series of Classification briefings. Subsequent briefings are strongly recommended but are optional. Managers may assign staff to take those additional subject-matter briefings based upon the topic's applicability to the areas associated with their work activities.

Resources

- ISS100.1.1, *Identify Classified Information*
- CLA102, *Classified Programs Initial Awareness Briefing*
- Classification website

End of Module Question

Howard is writing a report for DOE on a weapons program. Discussion with his DC indicates that it should be unclassified, and they have decided to treat it as programmatic. However, Howard subsequently decides to insert an unclassified article from an earlier unclassified paper. What risks is he taking?

a) None
b) He could be making the report classified.
c) He's committing plagiarism.
d) He risks incorporating information that has become obsolete.

Answer: b) Howard could be making the report classified.

Module 04 - Protection of Classified Information

Objective
After completing this module, you will be aware of the issues and requirements involving the protection of classified information.

Security Incidents
In 2009, there were 30 security incidents due to failure to properly store, handle, or disseminate classified information. The following list provides a few examples of how classified information can be compromised:

- Storing a classified document in a cabinet or desk drawer instead of the required GSA-approved safe or vault-type room (VTR).
- Holding classified discussions in hallways, break rooms, and rest rooms rather than behind closed doors within a Limited Area.
- Sharing classified information with cleared individuals without first disclosing that the information is classified and informing them of the level, category, and caveat (if any) of the information.
- Leaving a classified document in a classified printer.
- Allowing one's self to be distracted while engaged in locking or monitoring procedures.
- Failing to follow prescribed procedures when hand carrying a classified document.
- Discussing classified information on an unsecured line.
- Not thoroughly checking furniture (e.g., a desk or cabinet) for classified matter before removing it from a VTR.
- Failing to properly mark a classified document.
- Failing to seek classification guidance prior to initiating an e-mail related to a weapons program.
- Failing to review the entirety of an e-mail "string" to ensure that added information will not reveal classified information (referred to as "compilation").

Your Responsibility

You are responsible for ensuring that all classified information—whether it is written, verbal, or visual—is properly safeguarded from unauthorized access. Here are some processes to follow:

- Initiate and follow the two-person rule when performing locking and monitoring

procedures.
- Follow the two-person rule when removing furniture or containers from a VTR.
- Don't allow yourself to be distracted when working with classified matter.
- Use only secure (STE/STU) phones to discuss classified information.
- Consult with your Derivative Classifier (DC).
- Ensure that classified discussions are held in appropriate areas within a Limited Area.
- Do not make casual references to classified information. Identify the information as classified and ensure that the recipient of that information is appropriately cleared and has a "need to know."
- Work with your Classified Administrative Specialist (CAS). CASs are trained on the proper handling of classified information.

Consider posting an awareness message such as the chain link barrier pictured above.

Manager Responsibilities
Managers are responsible for:

- Ensuring that personnel within their organizations have received training commensurate with their security responsibilities.
- Informing new personnel of the security-related aspects of their duties and the resources available within the organization.

Resources

- ISS100.1, *Perform Classified Work*
- S&S-MAN-013, *Classified Workstations (CWS) Manual*
- Classified Matter Protection & Control (CMPC) website
- NEO200, *SNL ES&H, Safeguards & Security Orientation for Employees*
- NCO200, *SNL ES&H, Safeguards & Security Orientation for New SNL-Directed Contractors*
- SEC301, *Classified Matter Training*

End of Module Question

John is working on a draft of a classified paper when he receives a phone call informing him that he is late for a meeting. What should John do?

a) Temporarily store the papers in his desk drawer until he returns.
b) Leave the papers out but lock his office door.
c) Place all classified information back into the GSA-approved safe and lock it.

Answer: c) John should place all classified information back into the GSA-approved safe and lock it.

Module 05 - Vault-Type Rooms (VTRs) and Classified Repositories

Objectives
After completing this module, you will be aware of security concerns associated with VTRs and classified repositories, and of your responsibilities for ensuring they are properly used and secured.

Security Incidents
In FY09, there were 42 security incidents involving VTRs and classified repositories. Most of those incidents occurred because:

- Individuals failed to phone the Protective Force to set VTR alarms.
- Drawer, door, or dial was not checked according to security procedures.
- Non-residents were permitted unescorted access within a VTR.

Concern: Potential to Compromise Classified
Failing to protect classified information could lead to compromise of that information. Making assumptions that "nothing ever happens here," or that "everyone here is cleared," is contrary to good security practice. Always conduct activities involving classified matter with the thought in mind that anything is possible, and that, although individuals are cleared, they do not necessarily have the "need to know" required for access.

Your Responsibilities:

- Remain focused when performing locking and monitoring procedures.
- Ensure that only those individuals having "resident" status have unescorted access in a VTR.
- Ensure that individuals who perform locking and monitoring procedures are properly trained to conduct those activities. For information on training, refer to ISS100.1.10, *Manage Vaults and Vault-Type Rooms (V/VTRs)*.
- **Make no assumptions; seek assistance.**

Resources:

- SEC101VTR, *V/VTR User Training*: Required for all Members of the Workforce at SNL/NM who are on an access list for a vault or VTR. The requirement for

SEC101VTR is documented in ISS100.1.10, *Manage Vaults and Vault-Type Rooms (V/VTRs)*.

- SEC201VAD, *Training for VTR Custodians and VTR Managers*: Required for all at SNL/NM who function as a VTR Custodian (primary and alternate) and/or VTR Manager. The requirement for SEC201VAD is documented in S&S-MAN-028, *V/VTR Custodian Manual.*
- ISS100.1, *Perform Classified Work*.
- "Vault/Vault-Type Room (V/VTR) Services" (available at the Technical Security Systems website).
- S&S-MAN-013, *Classified Workstations (CWS) Manual*—contains information on monitoring procedures.

End of Module Question

John is in the middle of the process for locking a VTR. A coworker approaches, asking him to look at a report they're working on together. John should…

a) Stop what he's doing to review the report.
b) Explain to his coworker that he's locking the VTR, needs to remain focused, and the work must wait until he has completed his locking procedure.
c) Hurriedly go through the motions of locking the VTR so he can look at the report.

Answer: b) John should explain to his coworker that he's locking the VTR, needs to remain focused, and the work must wait until he has completed his locking procedure.

Module 06 - Controlled Articles

Objectives
The objective of this module is to increase your awareness of security issues associated with controlled articles and your responsibilities regarding those articles.

Security Incidents
In FY09, there were 473 security incidents involving controlled articles. The examples below show how making assumptions and deviating from required security practices can lead to security incidents.

- An uncleared individual, who keeps his cell phone in his pocket when in the Property Protection Area (PPA) where his office is located, attended a meeting in a Limited Area (LA)—with his phone in his pocket. The meeting had been hastily called, and the only room available was within the LA.
- Although asked every morning about controlled articles prior to entering the LA for meetings, an uncleared visitor forgot that the item was in the holster on his belt.
- A cleared individual failed to realize he was wearing his Bluetooth earpiece when he entered the LA.
- A cleared individual who was accustomed to carrying her cell phone in a specific place in her purse entered the LA with her cell phone. A family member who used the phone the previous day had returned it to a different location in the purse.

Concern: Compromise of Classified or Sensitive Information

Because they can record information, receive/transmit information, and/or be hacked into, controlled articles can be used as technical surveillance equipment, which can lead to the compromise of classified or sensitive information. Controlled articles include, but are not limited to:

- Cell phones
- Smart phones
- Bluetooth devices
- iPods
- Wireless keyboards
- Microphones
- Two-way pagers
- Cameras
- Music devices with recording capabilities

Your Responsibilities

You should always:

- Conduct a self-check prior to entering an LA or other area in which controlled articles are not permitted.
- Inform your uncleared and cleared visitors of security restrictions related to entering a security area.
- Ask visitors to conduct a self-check prior to entering security areas.
- Contact Physical Security prior to taking controlled articles into an LA.
- When in doubt about a controlled article, contact Physical Security for information and instructions.
- If you find you have introduced an unauthorized controlled or prohibited article, report it to your manager and/or SIMP immediately upon discovery.

The Safeguards and Security (S&S) program is striving to reduce cell phone incidents through a Cell Phone Band Awareness Campaign. Learn more about this campaign, and how to obtain cell phone bands at the Security BandIt page of the Security Education and Awareness Liaison (SEAL) website.

Resources

- Security Incident Management Program (SIMP)
- IM100.1.2, *Manage Controlled Electronic Devices and Media*
- ISS100.3.1, *Report Personnel Security Information; Security Incidents; and Waste, Fraud, and Abuse*
- ISS100.5.1, *Manage Controlled and Prohibited Articles*
- ISS100.5.2, *Conduct and Report Technical Surveillance*
- ISS100.5.3, *Control Site Access*
- Physical Security & Planning website
- controlledarticles@sandia.gov

End of Module Question

Jill is on her way to work, and is aware that she will arrive late for a meeting. She gets into her vehicle, attaches her Bluetooth earpiece, and calls the office to inform her manager that she's running late. Jill arrives at her building, which is an LA, swipes her badge, and begins to enter the building. What action did she fail to take prior to entering the LA?

a) No other action required.
b) Jill failed to conduct a self-check to verify that she did not have the Bluetooth device--or any other controlled or prohibited article--with her before entering the LA.

Answer: b) Jill failed to conduct a self-check to verify that she did not have the Bluetooth device--or any other controlled or prohibited article--with her before entering the LA.

Module 07 - Foreign Interactions

Objectives
After completing this module you will be aware of the following:

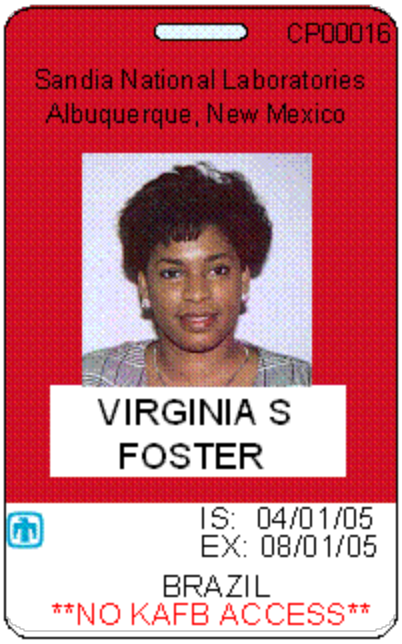
- Foreign national visits are strictly controlled.
- Associated responsibilities and procedures related to those visits.

Security Incidents
In FY09, there were seven security incidents involving hosting or escorting foreign nationals at SNL. These incidents were results of the host or escort making assumptions relative to what process could be followed for escorting or providing information to a foreign national.

Your Responsibilities
To host a foreign national visit, you must be an employee of Sandia or the Sandia Site Office (SSO), a U.S. citizen, be Q- or L-cleared, and possess a DOE-approved badge. A host must also have a current completion for International Business Practices training (FCPA100) and Export Control Awareness Training (EC100) recorded in his or her TEDS training notebook.

As host to an uncleared foreign national, you are responsible for:

- Ensuring that the benefit of the visit to SNL outweighs the potential risk.
- Ensuring that a Foreign National Request (FNR) Security Plan (SP) has been submitted and approved (per the time requirements) and is current. Coordinate any changes with the Foreign Interactions Office prior to the change.
- Understanding the requirement to brief any co-hosts or escorts of the information in the FNR SP.
- Ensuring that access to information is restricted to what is approved in the FNR SP.
- Identifying any unclassified area of your work that might be sensitive or might shed light on other work that is classified. Contact Operations Security (OPSEC) for assistance in identifying vulnerabilities.
- Assessing whether discussions of selected unclassified information with foreign nationals could divulge any proprietary details related to cooperative research or other collaborative work.
- Being aware that information deemed unclassified may also be export controlled.
- Ensuring that the foreign national's citizenship is correct in Enterprise Person.
- Ensuring that the original Lawful Status documentation is current and matches what is documented in the FNR SP.
- Adhering to all requirements listed in the Host Certification.



- Ensuring that the foreign national understands his or her responsibilities.
- Observing the FNR SP close-out procedures and returning badge(s) to the Badge Office.

An FNR SP must be approved before a foreign national may access any:

- Sandia-controlled premises.
- SNL information system resources.
- Sandia-controlled programs, information, or technologies that are not publicly available.

As an approved host, co-host, or escort you must:

- Be aware of, and strictly comply with, all the conditions listed on the FNR SP.
- Obtain prior approval before enacting any changes to the FNR SP.
- Ensure that the foreign national is escorted at all times while inside authorized limited or more restricted areas.
- Immediately report incidents of security concern involving foreign nationals to SIMP and implement the OOPS process.

Resources

- ISS100.4.1, *Control Access by Foreign Nationals to Unclassified DOE Information, Programs, and Technologies, and SNL Sites*
- ISS100.5.3, *Control Site Access*
- FCPA100, *International Business Practices*
- EC100, Export Control Awareness Training
- Operations Security (OPSEC) website
- Foreign Interactions website
- Host Certification and Risk Assessment
- DOE Sensitive Countries List

End of Module Question

Hosting a foreign national requires controls in addition to those implemented when hosting an uncleared U.S. citizen.

a) True
b) False

Answer: a) True. Hosting a foreign national requires controls in addition to those implemented when hosting an uncleared U.S. citizen.

Module 08 - HSPD-12 Federal Credential

Objective:
After completing this module, you will be familiar with:

- The security features of the HSPD-12 federal credential (badge).
- Your responsibilities regarding its use and protection.

Security Incidents:
In FY09 there were approximately 52 reports of lost or stolen badges. The number 52 may not seem significant for a population the size of SNL. However, every lost, stolen, and forgotten badge incident is of concern to DOE.

Security Features
Federal credentials, which are issued only by certified sources, can be immediately deactivated throughout the federal government. They have enhanced security features that make them more resistant to tampering, counterfeiting, theft, and terrorist exploitation. In the future, federal credentials will also be used to control access to federal computer systems.

Information Stored on the Credential
The credential displays a picture of your face; your last name, first name, and middle initial; a brief physical description (height, eye color, and hair color); agency; organization; and an expiration date. The credential also stores a personal identification number (PIN), two electronic fingerprints, and digital certificates for functions like authenticating the credential holder, digital signatures, and encrypting e-mail.

The badge holder that was issued to you has an electromagnetically opaque film that provides an additional layer of protection against unauthorized or unknown access to authentication information.

Your Responsibilities
It is your responsibility to use your credential as authorized.

- Use it only for official government purposes.
- Wear it only in government facilities.
- Have it with you at all times while at work. If you forget your credential, it is recommended that you go home and retrieve it. Otherwise, you must follow the steps

regarding a lost/stolen/forgotten badge, as required by ISS100.5.5, *Use, Control, and Protect Badges*.
- Replace it when it is damaged (e.g., your name is illegible) or when your picture no longer accurately represents you (e.g., does not show significant weight loss or gain since picture was taken).

Note: It will take approximately 2 weeks to obtain a new federal credential. If a new photo must be taken, you will need to schedule an appointment with a USAccess station to obtain another photo. You will be issued a site-specific badge until you receive your new federal credential.

You must protect your HSPD-12 federal credential and exercise the same care with it as you do with other identification (e.g., driver's license, passport). When not wearing your badge, leave it in a locked secure area.

- Protect your credential from loss or theft.
- Use only the badge holder that was issued to you with your HSPD-12 federal credential. Other holders damage and degrade the protective laminates on the credential.
- Do not mark on, punch holes in, or bend your credential.
- Damage to the credential's magnetic strip can be limited by using only the badge holder that was issued to you.
- Avoid subjecting your credential to excessive heat (e.g., by accidentally running it through the clothes dryer or leaving it on the dashboard in direct sunlight), as the credential might warp.
- Do not allow the credential near magnetic fields (e.g., stereo equipment, magnets, other magnetic-stripe cards).

Points about your PIN:

- Do not share your PIN.
- Protect your PIN number.
- If compromised, change your PIN.

Resources:

- ISS100.5.5, *Use, Control, and Protect Badges*
- Badge Office website

End of Module Question

Which of these is your responsibility?

a) Protect your HSPD-12 federal credential from damage.
b) Protect the credential from loss or theft.
c) Wear your credential at all times while at work.
d) All of the above.

Answer: d) All of the above are your responsibilities.

Module 09 - Clearance Transition

Objective
After completing this module, you will be aware of the DOE complex-wide initiative to decrease the number of DOE security clearances to:

- Verify that clearance levels are commensurate with a need to access the level and category of classified information based on each individual's current job assignment (e.g., a person with a Q clearance has need to access Secret Restricted Data [SRD] or higher).
- Reduce administrative expenses associated with obtaining and maintaining clearances.

Background
Clearance levels reflect only the ability to have access to specific classified information based on the current job assignment.

Q clearances cost more than 10 times as much as L clearances, and such expenses are borne by each national laboratory. Whereas almost all clearances at SNL have been at the Q level in the past, there is a transition underway toward an accurate and more cost-effective ratio of Q to L clearances. The DOE NNSA/Service Center, Personnel Security Department (PSD), will continue to process clearances that are needed to support mission work, commensurate with the level and category of the classified information accessed.

In principle, this DOE security clearance directive will ensure that Sandia pays for the clearances necessary to perform work in support of the mission and that the clearances are justifiable to DOE/NNSA.

Implementation of Transition
For those currently holding a DOE clearance, a re-determination of appropriate level of clearance will be made at the time of their routine reinvestigation, beginning with the FY10 reinvestigation schedule. Line management at SNL is responsible for reviewing an individual's current job assignments and duties when requesting a DOE security clearance, or when recertifying a clearance, to determine the appropriate clearance level (Q or L).

Justifications for clearance levels for new hires after FY09 will be based on the duties of their current job assignment. A clearance upgrade will be processed for an individual with an L clearance moving into a job assignment requiring a Q. According to DOE NNSA/Service Center, PSD, an individual's clearance can be upgraded from an L to a Q within 5 working days if both of the following apply:

- The individual previously held a Q clearance on the basis of a background investigation within the last 10 years.
- There is no unresolved derogatory information.

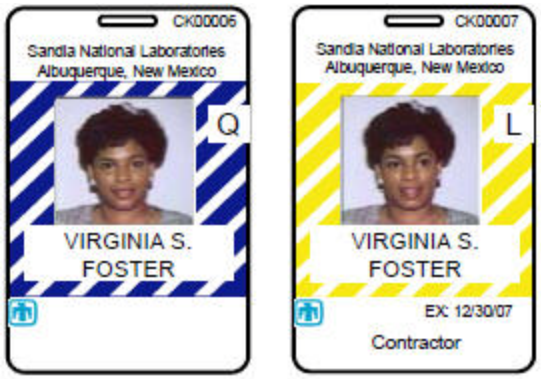
Changes to Security Environment
Generally, we have conducted mission work in Limited Areas under the assumption that all

personnel having unescorted access to the areas are Q-cleared. As a result of the clearance transition initiative, that will no longer be accurate. Therefore, some changes in workforce behavior will be required, including the following:

- For areas where a Q-clearance is required, including vault-type rooms (VTRs), L-cleared visitors must be escorted. Additional precautions must be taken to prevent their access—either visual or auditory—to SRD or higher classified information.
- Those who conduct meetings where SRD or higher material is presented or discussed should verify invitees' clearance levels prior to such meetings.
- Classified discussions at the SRD level should not take place in hallways within Limited Areas. Precautions should also be taken so that SRD discussions within an office cannot be overheard.
- When vouching (using your badge to allow others unescorted access to Sandia-controlled premises), a greater awareness of an individual's clearance becomes essential as the potential exists that someone who previously held a Q clearance and had access to an area may now possess an L clearance restricting his or her access to that area.

Distinguishing Clearance Levels Based on Badge Content

A site-specific badge has yellow stripes or blue stripes. Such badges are typically issued only on a temporary basis, pending issuance of an HSPD-12 federal credential for the cleared individual.



With respect to the HSPD-12 federal credential, it is more difficult to distinguish between a Q- and an L-clearance holder. Therefore, extra awareness is required to verify their level of clearance when admitting personnel to Q-only areas.

Resources

- ISS100.5.4, *Manage Clearances*
- SNL Personnel Access Authorization (Clearance) Principles
- Clearance Office website

End of Module Question

An Individual's clearance level should be based on level of access to classified information required for his/her current job assignment.

a) True
b) False

Answer: a) True**.** An individual's clearance level should be based on level of access to classified information required for his/her current job assignment.

SEC100 Feedback Form

Customer feedback is important to us. Please complete the evaluation form below and forward it to Course Administrator, MS1341, fax number (505) 284-6079.

Rate on a scale of 1- 5 (with 1= poor and 5 =excellent):

The ease of using of this learning tool and/or test? 1 2 3 4 5

The organization of information presented? 1 2 3 4 5

The amount of information presented? 1 2 3 4 5

The usefulness of the information presented? 1 2 3 4 5

Your level of knowledge related to this topic BEFORE using this learning tool and/or test?

1 2 3 4 5

Your level of knowledge related to this topic AFTER using this learning tool and/or test?

1 2 3 4 5

The overall quality of this learning tool and/or test? 1 2 3 4 5

Fill in the blanks:

What was most valuable about this learning tool or test?

_____

_____

_____

_____

What information needs to be corrected, inserted, removed, or updated?

_____

_____

_____

_____

What could be done to improve or enhance this learning tool or test?

_____

_____

_____

_____